Secure Transactio :An Credit Card Fraud Detection System Using Visual Cryptography

Prajakta Akole[1], Nikita Mane[2], Komal Shinde[3], Prof . Swati A. Khodke [4]

[123]Student of Computer Engineering, JSPM's BSIOTR College, Wagholi, Pune.

[4]Prof. Department of Computer Engineering, JSPM's BSIOTR College, Wagholi, Pune.

---***---

Abstract-*Today's world is Internet globe. Now a day popularity of E-commerce is increasing tremendously. Using E-commerce people do their financial deal online like online shopping etc. Most popular mode for online and offline payment is using credit card, use of credit card has significantly increased. So as credit card is becoming popular mode for online economic transactions, at the same time fraud associated with it are also rising. This paper describes a technique for secure transaction using visual cryptography. A new system is been proposed by using Visual Cryptography to Generate OTP for efficient and to reduce economic losses. The system is totally concerned with credit card application fraud detection by performing the process of visual cryptography. We propose an credit card fraud detection system that utilizes Visual Cryptography to Generate OTP for efficient transaction and to reduce economic losses. The system is totally concerned with credit card application fraud detection by performing the procedure of visual cryptography and grey scales to overwhelm the disadvantage mentioned previously in the existing systems. First, we have a tendency to Generate OTP image. For the OTP image we separate the RBG values and then we do grey scaling, the grey scaled image is given as an input for thresholding. Finally, shares are generated by (2,2)VCS.The experiment results show that our approach achieves affordable performance. Addresses the problem of password being vulnerable to attack, by OTP generation using visual cryptography secure transaction can be done efficiently..Today there isn't any search engine other than some of the above mention ones that provide a better responsiveness to the user's request for the result.*

Keywords: Grey scale; Thresholding algorithm ;OTP; Visual cryptography; Share Generation.

1. INTRODUCTION

In day to day living, online transactions are increased to purchase goods and services. According to Nielsen study conducted in 2007-2008, 28% of the world's total populace has been using internet [1].In developed countries and also in developing countries to some degree, credit card is most acceptable payment mode for online and offline transaction. As usage of credit card increase worldwide, chances of attacker to steal credit card details and then, make fraud transaction are also increasing. There are numerous ways to steal credit card details such as phishing websites, steal/lost credit cards, fake cards, theft of card details, intercepted cards etc[2].Now days, credit card transaction and online money transfer have been improved rapidly. Therefore, there is threat from third party or unauthorized party accessing secret information has been an still existing concern for the data communication experts. With the rapid advance in the system topology, multimedia data can be transmitting over the Internet conveniently. In order to deal with the security issue of credit card transaction, we are in need of an appropriate secure method of transaction by which we can secure our transaction over the internet. Credit card fraud detection system allows users to perform transaction securely using an OTP. The term one-time password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticate the user for a single transaction or session. An OTP is more safe than a static password, particularly a user-created password, which is typically weak. OTPs may replace confirmation login information or may be used in adding to it, to add another layer of security. OTP tokens are typically pocket-size fobs with a small screen that display a number. The number changes every 30 or 60 seconds, depending on how the token is configured.

In this paper, we propose an credit card fraud detection system based on the concept of Visual Cryptography for OTP.Visual cryptography is a cryptographic method which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a automatic operation that does not require a computer.

Visual Cryptography (VC) is one of the encryption method that is used to encrypt secret images in such a way that it can be decrypted by the individual visual system if the correct key images are used. The technique was first proposed by Moni Naor and Adi Shamir in 1994. According to them Image Cryptography is a method of encrypting a undisclosed image into shares such that stacking a adequate shares of secret image reveal the original image.[5] Shares are usually binary images existing in transparencies. Unlike, when compared to presented traditional cryptographic methods, Visual Cryptography needs no complicated calculation for recovering the secret image. The decryption method is to merely stacking the shares and view the original (secret) image that appear on the stack shares.[6]The method Visual Cryptography is being used for top secret transfer of images in military, hand written documents, text images.

The field of encryption is becoming very important in the present age in which information protection is of utmost concern. Security is an important issue in communication and storage of imagery, and encryption is one of the ways to ensure security. Image encryption has application in internet communication, multimedia systems, medical telemedicine, military communication, etc. Images are different from text. Although we may use the conventional cryptosystems to encrypt images directly, it is not a good idea for two reason. One is that the image size is almost for all time much greater than that of text. Therefore, the traditional cryptosystems require much time to directly encrypt the representation data. The other problem is that the decrypted text must be equal to the original transcript. However, this requirement is not required for image data. Due to the characteristic of human awareness, a decrypted image contain small distortion is usually acceptable.[4].Our goal is secure transaction by OTP generation using visual cryptography. For online transaction using credit card, we generate OTP using (2,2)VCS scheme which is not vulnerable to attack like the static password. The image is grey scaled the thresholding is done on grey image which gives the image with foreground and background colour. The thresholded image is divided into shares. Finally, the shares are superimposed to reveal the original image.

2. RELATED WORK

Visual Cryptography allows the well-organized and effective secret sharing between the number of trusted parties. As per concern the , trust is the most difficult part in many cryptographic schemes. It provides a powerful technique by which one secret can be spread into two or more shares. When the shares Xeroxed onto transparencies and then it can be superimposed accurately together so the original secret can be discovered without any computer participation. The complexity facing is the contrast of reconstructed image is not maintained and also the additional processing required for colored images[7].Visual cryptography has attracted the attention of many researchers in the recent past. Many authors focused their attention on different Visual Cryptography Schemes for different applications. Each scheme has its own advantages and disadvantages. Noar and Shamir have worked on basic Visual Cryptography Scheme. Without complex calculations, it can restore encrypted messages by stack two shares via human visual system. The first visual cryptography scheme is used for the black-and-white image. Every pixel is sub separated into 4 sub pixels into two shares. Share 1 is a key and share 2 is assumed to be secret message. The sub pixels of the share are aligned using XOR to get half black pixel and full black pixels The chosen random cell is a key. Share 1 does not provide any information. The cipher share2 is generated by choosing corresponding cell for black sub pixel and same cell for white sub pixel. Then two shares are stacked to extract the original information[8].

3. PROPOSED ALGORITHM

A. *Design Considerations*:

- Gray scaling of image.
- Thresholding of image.
- Visual Cryptography.
- Share Generation.

B. *Description of the Proposed Algorithm:*

Aim of the proposed algorithm is secure credit card transaction by OTP Generation using Visual Cryptography. The proposed algorithm consists of two main parts .

Step 1: OTP:

A one-time password (OTP) is an automatically generate numeric or alphanumeric string of characters that authenticates the user for a single session .A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer structure or other digital device. OTPs avoid a number of shortcomings that are associated with habitual (static) password-base authentication; a number of implementations also incorporate two factor verification by ensure that the one-time password requires access to something a person has (such as a small key ring fob machine with the OTP calculator build into it, or a smartcard or specific cell phone) as well as incredible a person knows (such as a PIN).

The most important advantage that is address by OTPs is that, in contrast to static passwords, they are not exposed to replay attacks. This means that a potential intruder who manages to record an OTP that was previously used to register into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major profit is that a user who uses the same (or similar) password for multiple systems, is not made susceptible on all of them, if the password for one of these is gained by an attacker.

OTP tokens are frequently pocket-size fobs with a small screen that display a number. The number changes every 30 or 60 seconds, depending on how the symbol is configured. For two-factor authentication, the user enter his user ID, PIN and the OTP to access the system.

Step 2: Visual Cryptography:

In order to transmit secret image to other people, a variety of encryption schemes have been proposed. Even with the remarkable progress of computer technology, using a computer to decrypt secrets is infeasible in some situations. For an example, consider a bank vault that must be open every day by five tellers, but for security purposes it is desirable not to trust any two individuals with the combination. Hence, a vault-access system that requires any three of the five tellers may be desirable. In this situation the traditional cryptography systems fail because they need to verify the five teller or 3 of them at a time using single key.[5] It refers to method for distributing a secret among a group of participant, each of whom is allocated a share of the secret. The secret can be reconstructed only when sufficient number of shares is combined individual shares are of no use on their own. In Secret Sharing Scheme, both the sharing phase and the rebuilding phase involve algorithms that are run by computers (specially, a dealer runs a distribution algorithm and a set of capable parties can run a reconstruction algorithm). In Visual Secret Sharing Scheme, the decryption stage needs no computer power but it has all the properties of Secret Sharing Schemes.

Visual cryptography was pioneer by Moni Naor and Adi Shamir in 1994. They established a visual secret sharing scheme, where an image was shifting into n shares so that only somebody with all n shares could decrypt the image, while any n-1 shares exposed no information about the original image. Each share was in print on a separate transparency, and decryption was performed by overlay the shares. When all n shares were overlay, the original image would appear. Visual cryptography is a new technique which provide information security which uses simple algorithm unlike the complex, computationally exhaustive algorithms used in other technique like Traditional cryptography. This technique allows Visual in turn (pictures, text, etc) to be encrypted in such a method that their decryption can be performed by the human visual system, without any difficult cryptographic algorithms. [4].

The following subsections describe methods for OTP generation using visual cryptography:

3.1 Gray Scale

In a (8-bit) grayscale image all picture element has an assigned intensity that ranges from 0 to 255.A grey scale image is unlike from black and white image since a grayscale image also include shades of grey distant from unadulterated black and pure white color. Grayscale images are generally required for image processing. To transform a colour image into gray scale we use gray scaling algorithm. Each colour pixel is described by a triple (R, G, B) intensities for red, green and blue, we have to map that to a single number giving a grayscale value.

Calculate grayscale component(R + G + B) / 3

Fig-1:Color – Grayscale

3.2 Thresholding of Image

Thresholding is the simplest process of image segmentation. From a grayscale image, thresholding can be used to create binary images i.e. image with just black or white colors. It is usually used for feature extraction where required features of image are transformed to white and everything else to black. (or vice-versa). It is an image processing technique for converting a grayscale to a binary image based upon a threshold value. If a pixel in the image has a gray level value which is less than the threshold value, the corresponding pixel in the resultant image is set to be black or else, if the gray scale of the pixel is greater than or equal to the threshold intensity, the resulting pixel is set to be white. Thus creating an image with only 2 colors. Image Thresholding is very useful for keeping the significant part of an image and getting rid of distorted image caused by noise.

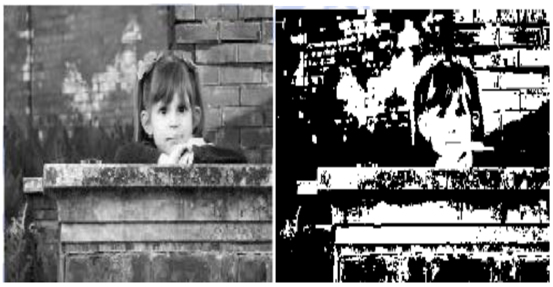


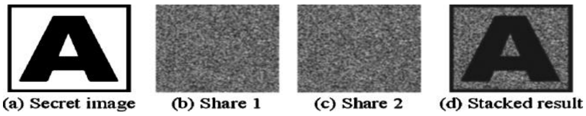
Fig-2:Grayscale – Threshold

3.3 Visual Cryptography

It is a kind of secret sharing scheme that focuses on sharing secret images. The basic idea of the visual cryptography scheme is to split a secret image into number of casual shares (printed on transparencies) which separately reveals no data about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the shares.[9]Visual Cryptography uses two transparent images. One image contains random pixels and the other image contain the secret information. It is impossible to retrieve the secret information from one of the images.[8]

3.4 Share Generation (2,2) Threshold VCS scheme

This is a simplest threshold scheme that take a secret message and encrypts it in two different shares that reveal the secret image when they are overlay. No additional information is required to create this kind of access structure.[9]In the case of (2, 2) VCS, each pixel P in the unique image is encrypted into two sub pixels called shares. Note that the selection of shares for a white and a black pixel is randomly determined. Neither share provides any clue about the original pixel as different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimpose, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we obtain one black sub pixel and one white sub pixel.



(a) Secret image (b) Share 1 (c) Share 2 (d) Stacked result

Fig 3. Share Generation

- RGB TO GREY SCALE ALGORITHM

Input: Colour Image

Output: Greyscale Image

1. Traverse through entire input image array.

2. Examine each pixel color value (24-bit).

3. Split the color value into each R, G and B 8-bit values

4. Calculate the grayscale part (8-bit)

forgiven R, G and B pixels using a

alteration formula.

5. Compose a 24-bit pixel value beginning

8-bit gray scale value.

6. Store the new value at same place in output

```
return
end if
end if
```

- THRESHOLDING ALGORITHM

Input: Grey scale image.

Output: Thresholded image

1. Traverse through entire input image array

2. Examine each pixel color value (24-bit) and alter it into grayscale.

3. Calculate the binary output pixel rate (black or white) based on existing threshold.

4. Store the new value at same position in output image.

5. Thresholding Logic

```
    GS = (r+g+b) / 3; // grayscale
    if(GS < th) {
    pix = 0; // pure black
    }
    else
    {
    pix = 0xFFFFFF; // pure white
    }
```

6. Store the new value at same place in output.

4. SIMULATION RSESULT

The process begins by browsing the products then select the products, enter transaction details when the details enter are correct process transaction if the details are wrong OTP generation.OTP image is greyscaled then thresholding is done. Visual Cryptography is done to generate shares. One share is send through the network And other appears on GUI. The share which is send through network is uploaded an both shares are superimopsed to reveal the original OTP image.OTP is verified and then payment is successfully done.

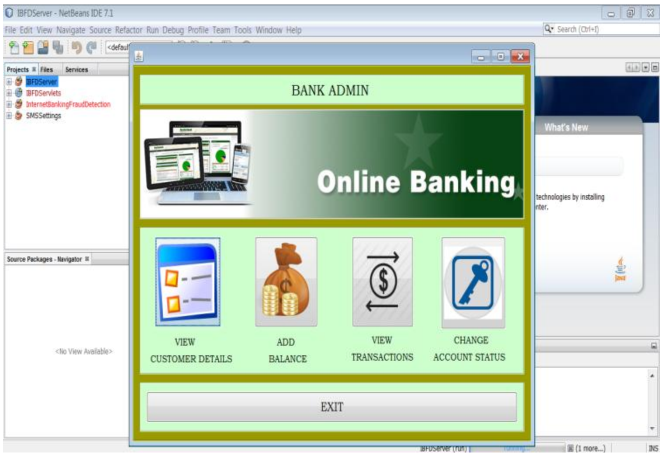


Fig-5:Admin module

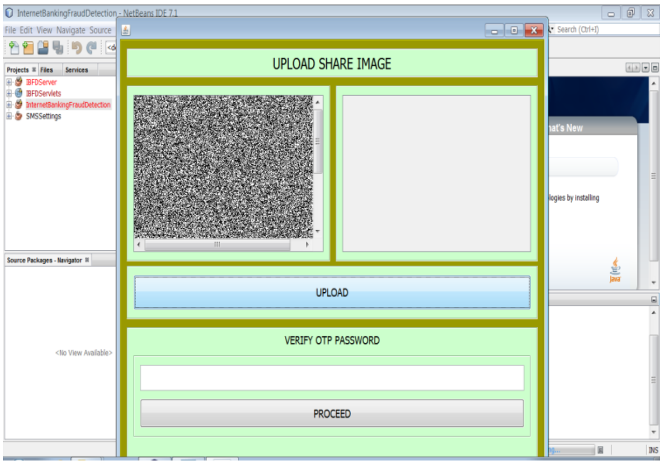
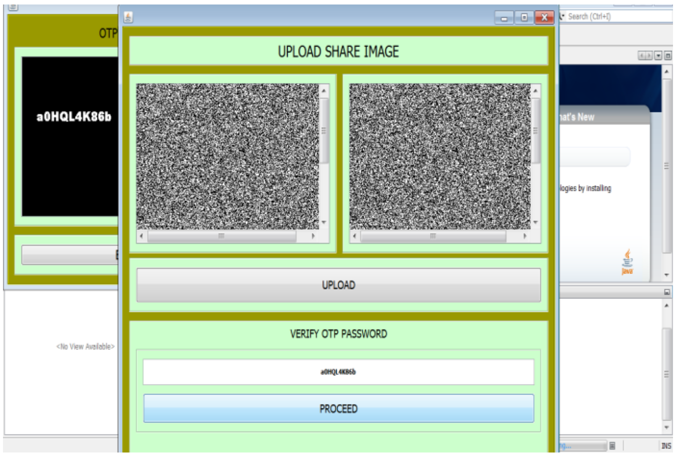


Fig-6:Generated Shares



a0HQL4K86b

a0HQL4K86b

Fig-7:Uploaded Shares for verification

5. CONCLUSION

In this paper, we have proposed an Credit Card fraud detection system based on the concept of OTP generation using Visual Cryptography [1]. The proposed system utilizes Visual Cryptography to generate OTP using share generation to overcome the disadvantage exhibited by the credit card fraud detection system using threshold value calculation. This system has been introduced as a trade off balance between security and convenience. If the level of security increases, the level of convenience decreases and vice versa.The VCS model described is very useful in providing mutual authentication among a group of participants as a whole.

REFERENCE

[1]Internet world usage (http://www.internetworldstats.com/stats.htm) (2011).

[2] V. Bhusari, S. Patil, "Application of Hidden Markov Model in Credit Card Fraud Detection," International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.6, November 2011

[3] Divya James, Mintu Philip,"A Novel Anti Phishing framework based on Visual Cryptography," in Proceedings of Power, Signals, Controls and Computation (EPSCICON), 2012.

[4] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Securing Images Using Colour Visual Cryptography and Wavelets,, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3, March 2012.

[5] Moni Naor and Adi Shamir, "Visual cryptography," In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, 1995, (950):pp. 1-12

[6] Ranjan Kumar H S, Prasanna Kumar H R, Sudeepa K B and Ganesh Aithal, "Enhanced Security System using Symmetric Encryption and Visual Cryptography," International Journal of Advances in Engineering &Technology ©IJAET, Vol. 6, Issue 3, pp. 1211-1219, July 2013, ISSN: 22311963.

[7] Mrs.Nidhina.K, Mr.P.Manikandan,"Extended Visual cryptography SchemeInternational Journal On Engineering Technology and Sciences," IJETS™ ISSN (P): 2349-3968, ISSN (O): 2349-3976 Volume 2 - Issue 5, May 2015.

[8] Dr. Ch. Samson,Masabattula N S S Durgamba, "Multiple Image Sharing Scheme using Visual Cryptography," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 8, August 2015.

[9] Mr.Thorat N.N , Mr.Patil P.P, Prof.Thakur Ritesh ,Ms.Kiranmai B, "Visual Cryptography Schemes for Secret Colour Images Sharing," Ijret Vol.2 - Issue 11 (November - 2013)